Vulnerability Summary for the Week of July 5, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 07/12/2021 12:06 PM EDT

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of July 5, 2021

07/12/2021 08:18 AM EDT

Original release date: July 12, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artware_cms_project -- artware_cms	ARTWARE CMS parameter of image upload function does not filter the type of upload files which allows remote attackers can upload arbitrary files without logging in, and further execute code unrestrictedly.	2021-07-07	7.5	CVE-2021-32538 CONFIRM
beardev -- joomsport	The joomsport_md_load AJAX action of the JoomSport WordPress plugin before 5.1.8, registered for both unauthenticated and unauthenticated users, unserialised user input from the shattr POST parameter, leading to a PHP Object Injection issue. Even though the plugin does not have a suitable gadget chain to exploit this, other installed plugins could, which might lead to more severe issues such as RCE	2021-07-06	7.5	CVE-2021-24384 CONFIRM
commscope -- ruckus_iot_controller	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Hard-coded System Passwords that provide shell access.	2021-07-07	10	CVE-2021-33218 MISC MISC
commscope -- ruckus_iot_controller	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The Web Application allows Arbitrary Read/Write actions by authenticated users. The API allows an HTTP POST of arbitrary content into any file on the filesystem as root.	2021-07-07	9	CVE-2021-33217 MISC MISC
commscope -- ruckus_iot_controller	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Unauthenticated API Endpoints.	2021-07-07	7.5	CVE-2021-33221 MISC MISC
commscope -- ruckus_iot_controller	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. There are Hard-coded Web Application Administrator Passwords for the admin and nplus1user accounts.	2021-07-07	7.5	CVE-2021-33219 MISC MISC
commscope -- ruckus_iot_controller	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. An Undocumented Backdoor exists, allowing shell access via a developer account.	2021-07-07	7.5	CVE-2021-33216 MISC MISC
djangoproject -- django	Django 3.1.x before 3.1.13 and 3.2.x before 3.2.5 allows QuerySet.order_by SQL injection if order_by is untrusted input from a client of a web application.	2021-07-02	7.5	CVE-2021-35042 MISC CONFIRM MISC CONFIRM
just-safe-set_project -- just-safe-set	Prototype pollution vulnerability in 'just-safe-set' versions 1.0.0 through 2.2.1 allows an attacker to cause a denial of service and may lead to remote code execution.	2021-07-07	7.5	CVE-2021-25952 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kaseya -- vsa	Kaseya VSA before 9.5.7 allows credential disclosure, as exploited in the wild in July 2021.	2021-07-09	7.5	CVE-2021-30116 MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. Autoblocks for CentralAuth-issued suppression blocks are not properly implemented.	2021-07-02	7.5	CVE-2021-36128 MISC MISC MISC
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension in MediaWiki through 1.36. If the MediaWiki:Abusefilter-blocker message is invalid within the content language, the filter user falls back to the English version, but that English version could also be invalid on a wiki. This would result in a fatal error, and potentially fail to block or restrict a potentially nefarious user.	2021-07-02	7.5	CVE-2021-36126 MISC MISC
microsoft -- windows_10	Windows Print Spooler Remote Code Execution Vulnerability	2021-07-02	9	CVE-2021-34527 MISC
ninjateam -- video_downloader_for_tiktok	Server-side request forgery in the Video Downloader for TikTok (aka downloader-tiktok) plugin 1.3 for WordPress lets an attacker send crafted requests from the back-end server of a vulnerable web application via the njt-tk-download-video parameter. It can help identify open ports, local network hosts and execute command on services	2021-07-07	7.5	CVE-2020-24142 MISC
phplist -- phplist	Remote Code Execution vulnerability in phplist 3.5.1. The application does not check any file extensions stored in the plugin zip file, Uploading a malicious plugin which contains the php files with extensions like PHP,phtml,php7 will be copied to the plugins directory which would lead to the remote code execution	2021-07-06	7.5	CVE-2020-22249 MISC
profilepress -- wp-user-avatar	A vulnerability in the file uploader component found in the ~/src/Classes/FileUploader.php file of the ProfilePress WordPress plugin made it possible for users to upload arbitrary files during user registration or during profile updates. This issue affects versions 3.0.0 - 3.1.3. .	2021-07-07	7.5	CVE-2021-34624 MISC
profilepress -- wp-user-avatar	A vulnerability in the user registration component found in the ~/src/Classes/RegistrationAuth.php file of the ProfilePress WordPress plugin made it possible for users to register on sites as an administrator. This issue affects versions 3.0.0 - 3.1.3. .	2021-07-07	7.5	CVE-2021-34621 MISC
profilepress -- wp-user-avatar	A vulnerability in the image uploader component found in the ~/src/Classes/ImageUploader.php file of the ProfilePress WordPress plugin made it possible for users to upload arbitrary files during user registration or during profile updates. This issue affects versions 3.0.0 - 3.1.3. .	2021-07-07	7.5	CVE-2021-34623 MISC
qsan -- sanos	Command injection vulnerability in QSAN XEVO, SANOS allows remote unauthenticated attackers to execute arbitrary commands.	2021-07-07	7.5	CVE-2021-32529 CONFIRM
qsan -- sanos	The QSAN SANOS setting page does not filter special parameters. Remote attackers can use this vulnerability to inject and execute arbitrary commands without permissions.	2021-07-07	7.5	CVE-2021-32533 CONFIRM
qsan -- sanos	QSAN SANOS factory reset function does not filter special parameters. Remote attackers can use this vulnerability to inject and execute arbitrary commands without permissions.	2021-07-07	7.5	CVE-2021-32534 CONFIRM
qsan -- sanos	The vulnerability of hard-coded default credentials in QSAN SANOS allows unauthenticated remote attackers to obtain administrator’s permission and execute arbitrary functions.	2021-07-07	7.5	CVE-2021-32535 CONFIRM
qsan -- sanos	Use of MAC address as an authenticated password in QSAN Storage Manager, XEVO, SANOS allows local attackers to escalate privileges.	2021-07-07	7.5	CVE-2021-32521 CONFIRM
qsan -- storage_manager	The same hard-coded password in QSAN Storage Manager's in the firmware allows remote attackers to access the control interface with the administrator’s credential, entering the hard-coded password of the debug mode to execute the restricted system instructions.	2021-07-07	9	CVE-2021-32525 CONFIRM
qsan -- storage_manager	Use of hard-coded cryptographic key vulnerability in QSAN Storage Manager allows attackers to obtain users’ credentials and related permissions.	2021-07-07	7.5	CVE-2021-32520 CONFIRM
qsan -- storage_manager	QuickInstall in QSAN Storage Manager does not filter special parameters properly that allows remote unauthenticated attackers to inject and execute arbitrary commands.	2021-07-07	7.5	CVE-2021-32512 CONFIRM
qsan -- storage_manager	QsanTorture in QSAN Storage Manager does not filter special parameters properly that allows remote unauthenticated attackers to inject and execute arbitrary commands.	2021-07-07	7.5	CVE-2021-32513 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qsan -- xevo	OS command injection vulnerability in Array function in QSAN XEVO allows remote unauthenticated attackers to execute arbitrary commands via status parameter.	2021-07-07	7.5	CVE-2021-32530 CONFIRM
qsan -- xevo	OS command injection vulnerability in Init function in QSAN XEVO allows remote attackers to execute arbitrary commands without permissions.	2021-07-07	7.5	CVE-2021-32531 CONFIRM
record-like-deep-assign_project -- record-like-deep-assign	All versions of package record-like-deep-assign are vulnerable to Prototype Pollution via the main functionality.	2021-07-02	7.5	CVE-2021-23402 CONFIRM CONFIRM
splinterware -- system_scheduler	Splinterware System Scheduler Professional version 5.30 is subject to insecure folders permissions issue impacting where the service 'WindowsScheduler' calls its executable. This allow a non-privileged user to execute arbitrary code with elevated privileges (system level privileges as "nt authority\system") since the service runs as Local System.	2021-07-06	7.2	CVE-2021-31771 MISC MISC MISC
stockware -- motor	Lack of authentication or validation in motor_load_more, motor_gallery_load_more, motor_quick_view and motor_project_quick_view AJAX handlers of the Motor WordPress theme before 3.1.0 allows an unauthenticated attacker access to arbitrary files in the server file system, and to execute arbitrary php scripts found on the server file system. We found no vulnerability for uploading files with this theme, so any scripts to be executed must already be on the server file system.	2021-07-06	7.5	CVE-2021-24375 MISC CONFIRM
ts-nodash_project -- ts-nodash	All versions of package ts-nodash are vulnerable to Prototype Pollution via the Merge() function due to lack of validation input.	2021-07-02	7.5	CVE-2021-23403 MISC MISC
zyxel -- usg1900_firmware	An authentication bypasss vulnerability in the web-based management interface of Zyxel USG/Zywall series firmware versions 4.35 through 4.64 and USG Flex, ATP, and VPN series firmware versions 4.35 through 5.01, which could allow a remote attacker to execute arbitrary commands on an affected device.	2021-07-02	7.5	CVE-2021-35029 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accusoft -- imagegear	An integer overflow vulnerability exists in the DICOM parse_dicom_meta_info functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to a stack-based buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	2021-07-07	6.8	CVE-2021-21807 MISC
alpinelinux -- aports	In the xrdp package (in branches through 3.14) for Alpine Linux, RDP sessions are vulnerable to man-in-the-middle attacks because pre-generated RSA certificates and private keys are used.	2021-07-05	4.3	CVE-2021-36158 MISC
apache -- druid	In the Druid ingestion system, the InputSource is used for reading data from a certain data source. However, the HTTP InputSource allows authenticated users to read data from other sources than intended, such as the local file system, with the privileges of the Druid server process. This is not an elevation of privilege when users access Druid directly, since Druid also provides the Local InputSource, which allows the same level of access. But it is problematic when users interact with Druid indirectly through an application that allows users to specify the HTTP InputSource, but not the Local InputSource. In this case, users could bypass the application-level restriction by passing a file URL to the HTTP InputSource.	2021-07-02	4	CVE-2021-26920 MISC MLIST MLIST
apache -- jena_fuseki	A vulnerability in the HTML pages of Apache Jena Fuseki allows an attacker to execute arbitrary javascript on certain page views. This issue affects Apache Jena Fuseki from version 2.0.0 to version 4.0.0 (inclusive).	2021-07-05	4.3	CVE-2021-33192 MISC
chimpgroup -- foodbakery	The WP Foodbakery WordPress plugin before 2.2, used in the FoodBakery WordPress theme before 2.2 did not properly sanitize the foodbakery_radius parameter before outputting it back in the response, leading to an unauthenticated Reflected Cross-Site Scripting (XSS) vulnerability.	2021-07-06	4.3	CVE-2021-24389 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cminds -- cm_download_manager	Cross Site Scripting (XSS) vulnerability in the CM Download Manager (aka cm-download-manager) plugin 2.7.0 for WordPress allows remote attackers to inject arbitrary web script or HTML via a crafted deletescreenshot action.	2021-07-07	4.3	CVE-2020-24145 MISC MISC
codemiq -- wordpress_email_template_designer	Cross-site request forgery (CSRF) vulnerability in WordPress Email Template Designer - WP HTML Mail versions prior to 3.0.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-07	6.8	CVE-2021-20779 MISC MISC MISC
commscope -- ruckus_iot_controller	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. The API allows Directory Traversal.	2021-07-07	4	CVE-2021-33215 MISC MISC
commscope -- ruckus_iot_controller	An issue was discovered in CommScope Ruckus IoT Controller 1.7.1.0 and earlier. Hard-coded API Keys exist.	2021-07-07	4.6	CVE-2021-33220 MISC MISC
contempothemes -- real_estate_7	The WP Pro Real Estate 7 WordPress theme before 3.1.1 did not properly sanitise the ct_community parameter in its search listing page before outputting it back in it, leading to a reflected Cross-Site Scripting which can be triggered in both unauthenticated or authenticated user context	2021-07-06	4.3	CVE-2021-24387 CONFIRM MISC
deltaww -- dopsoft	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to disclose information.	2021-07-02	4.3	CVE-2021-27455 MISC
deltaww -- dopsoft	Delta Electronics DOPSoft Versions 4.0.10.17 and prior are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code.	2021-07-02	6.8	CVE-2021-27412 MISC
elecom -- wrc-300febk_firmware	WRC-300FEBK, WRC-F300NF, WRC-733FEBK, WRH-300RD, WRH-300BK, WRH-300SV, WRH-300WH, WRH-H300WH, WRH-H300BK, WRH-300BK-S, and WRH-300WH-S all versions allows an unauthenticated network-adjacent attacker to execute an arbitrary OS command via unspecified vectors.	2021-07-07	5.8	CVE-2021-20739 MISC MISC
export_users_with_meta_project -- export_users_with_meta	The Export Users With Meta WordPress plugin before 0.6.5 did not escape the list of roles to export before using them in a SQL statement in the export functionality, available to admins, leading to an authenticated SQL Injection.	2021-07-06	6.5	CVE-2021-24451 CONFIRM
flask-user_project -- flask-user	This affects all versions of package Flask-User. When using the make_safe_url function, it is possible to bypass URL validation and redirect a user to an arbitrary URL by providing multiple back slashes such as /////evil.com/path or \\evil.com/path. This vulnerability is only exploitable if an alternative WSGI server other than Werkzeug is used, or the default behaviour of Werkzeug is modified using 'autocorrect_location_header=False.	2021-07-05	5.8	CVE-2021-23401 MISC MISC MISC
fluentforms -- contact_form	The WP Fluent Forms plugin < 3.6.67 for WordPress is vulnerable to Cross-Site Request Forgery leading to stored Cross-Site Scripting and limited Privilege Escalation due to a missing nonce check in the access control function for administrative AJAX actions	2021-07-07	6.8	CVE-2021-34620 MISC MISC
fortinet -- fortiauthenticator	Usage of hard-coded cryptographic keys to encrypt configuration files and debug logs in FortiAuthenticator versions before 6.3.0 may allow an attacker with access to the files or the CLI configuration to decrypt the sensitive data, via knowledge of the hard-coded key.	2021-07-06	5	CVE-2021-24005 CONFIRM
gitlab -- gitlab	A cross-site request forgery vulnerability in the GraphQL API in GitLab since version 13.12 and before versions 13.12.6 and 14.0.2 allowed an attacker to call mutations as the victim	2021-07-07	4.3	CVE-2021-22224 MISC CONFIRM MISC
gitlab -- gitlab	An information disclosure vulnerability in GitLab EE versions 13.10 and later allowed a user to read project details	2021-07-07	4	CVE-2021-22233 MISC CONFIRM
gitlab -- gitlab	Client-Side code injection through Feature Flag name in GitLab CE/EE starting with 11.9 allows a specially crafted feature flag name to PUT requests on behalf of other users via clicking on a link	2021-07-06	4.3	CVE-2021-22223 CONFIRM MISC MISC
gitlab -- gitlab	A reflected cross-site script vulnerability in GitLab before versions 13.11.6, 13.12.6 and 14.0.2 allowed an attacker to send a malicious link to a victim and trigger actions on their behalf if they clicked it	2021-07-07	4.3	CVE-2021-22227 MISC CONFIRM MISC
gitlab -- gitlab	An issue has been discovered in GitLab affecting all versions. Improper access control allows unauthorised users to access project details using Graphql.	2021-07-06	4	CVE-2021-22228 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	Improper code rendering while rendering merge requests could be exploited to submit malicious code. This vulnerability affects GitLab CE/EE 9.3 and later through 13.11.6, 13.12.6, and 14.0.2.	2021-07-07	6.5	CVE-2021-22230 MISC CONFIRM
gitlab -- gitlab	Under certain conditions, some users were able to push to protected branches that were restricted to deploy keys in GitLab CE/EE since version 13.9	2021-07-06	4.9	CVE-2021-22226 MISC CONFIRM
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.8. Under a special condition it was possible to access data of an internal repository through project fork done by a project member.	2021-07-06	4.3	CVE-2021-22229 MISC CONFIRM
gitlab -- gitlab	A denial of service in user's profile page is found starting with GitLab CE/EE 8.0 that allows attacker to reject access to their profile page via using a specially crafted username.	2021-07-07	4	CVE-2021-22231 MISC MISC CONFIRM
google -- chrome	Use after free in WebAudio in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-07-02	6.8	CVE-2021-30556 MISC MISC GENTOO
google -- chrome	Use after free in TabGroups in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	2021-07-02	6.8	CVE-2021-30557 MISC MISC GENTOO
google -- chrome	Use after free in Sharing in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page and user gesture.	2021-07-02	6.8	CVE-2021-30555 MISC MISC GENTOO
google -- chrome	Use after free in WebGL in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-07-02	6.8	CVE-2021-30554 MISC MISC GENTOO
gvectors -- wpforo_forum	The wpForo Forum WordPress plugin before 1.9.7 did not validate the redirect_to parameter in the login form of the forum, leading to an open redirect issue after a successful login. Such issue could allow an attacker to induce a user to use a login URL redirecting to a website under their control and being a replica of the legitimate one, asking them to re-enter their credentials (which will then in the attacker hands)	2021-07-06	5.8	CVE-2021-24406 CONFIRM
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 3.0.0.3 and 4.0.0.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195711.	2021-07-07	5	CVE-2021-20379 CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 4.0.0.4 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 196217.	2021-07-07	5	CVE-2021-20415 CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 3.0.0.3 and 4.0.0.4 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 196218.	2021-07-07	5	CVE-2021-20416 CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 4.0.0.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196219	2021-07-07	4	CVE-2021-20417 CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 3.0.0.2 and 4.0.0.4 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 195709.	2021-07-07	6.5	CVE-2021-20378 CONFIRM XF
icewarp -- webclient	Cross Site Scripting (XSS) in Webmail Calender in IceWarp WebClient 10.3.5 allows remote attackers to inject arbitrary web script or HTML via the "p4" field.	2021-07-07	4.3	CVE-2020-25925 MISC
izsoft -- easy_cookies_policy	The Easy Cookies Policy WordPress plugin through 1.6.2 is lacking any capability and CSRF check when saving its settings, allowing any authenticated users (such as subscriber) to change them. If users can't register, this can be done through CSRF. Furthermore, the cookie banner setting is not sanitised or validated before being output in all pages of the frontend and the backend settings one, leading to a Stored Cross-Site Scripting issue.	2021-07-06	4	CVE-2021-24405 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
j2global -- myfax	myFax version 229 logs sensitive information in the export log module which allows any user to access critical information.	2021-07-07	4	CVE-2020-24038 MISC MISC
joomla -- joomla\!	An issue was discovered in Joomla! 3.0.0 through 3.9.27. Inadequate escaping in the rules field of the JForm API leads to a XSS vulnerability.	2021-07-07	4.3	CVE-2021-26035 MISC
joomla -- joomla\!	An issue was discovered in Joomla! 3.0.0 through 3.9.27. Inadequate escaping in the imagelist view of com_media leads to a XSS vulnerability.	2021-07-07	4.3	CVE-2021-26039 MISC
joomla -- joomla\!	An issue was discovered in Joomla! 2.5.0 through 3.9.27. Missing validation of input could lead to a broken usergroups table.	2021-07-07	5	CVE-2021-26036 MISC
joomla -- joomla\!	An issue was discovered in Joomla! 2.5.0 through 3.9.27. CMS functions did not properly termine existing user sessions when a user's password was changed or the user was blocked.	2021-07-07	5	CVE-2021-26037 MISC
joomla -- joomla\!	An issue was discovered in Joomla! 2.5.0 through 3.9.27. Install action in com_installer lack the required hardcoded ACL checks for superusers. A default system is not affected cause the default ACL for com_installer is limited to super users already.	2021-07-07	4.3	CVE-2021-26038 MISC
linux -- acrn	ACRN before 2.5 has a devicemodel/hw/pci/xhci.c NULL Pointer Dereference for a trb pointer.	2021-07-02	5	CVE-2021-36146 MISC
linux -- acrn	ACRN before 2.5 has a hw/pci/virtio/virtio.c vq_endchains NULL Pointer Dereference.	2021-07-02	5	CVE-2021-36143 MISC
linux -- acrn	An issue was discovered in ACRN before 2.5. It allows a devicemodel/hw/pci/virtio/virtio_net.c virtio_net_ping_rxq NULL pointer dereference for vq->used.	2021-07-02	5	CVE-2021-36147 MISC
linux -- acrn	The polling timer handler in ACRN before 2.5 has a use-after-free for a freed virtio device, related to devicemodel/hw/pci/virtio/*.c.	2021-07-02	5	CVE-2021-36144 MISC
linux -- acrn	The Device Model in ACRN through 2.5 has a devicemodel/core/mem.c use-after-free for a freed rb_entry.	2021-07-02	5	CVE-2021-36145 MISC
linux -- acrn	An issue was discovered in ACRN before 2.5. dmar_free_irte in hypervisor/arch/x86/vtd.c allows an irte_alloc_bitmap buffer overflow.	2021-07-02	6.8	CVE-2021-36148 MISC
linux -- linux_kernel	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space	2021-07-07	4.6	CVE-2021-22555 MISC MISC MISC
media_file_organizer_project -- media_file_organizer	Directory traversal in the Media File Organizer (aka media-file-organizer) plugin 1.0.1 for WordPress lets an attacker get access to files that are stored outside the web root folder via the items[] parameter in a move operation.	2021-07-07	5	CVE-2020-24144 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the Translate extension in MediaWiki through 1.36. The Aggregategroups Action API module does not validate the parameter for aggregategroup when action=remove is set, thus allowing users with the translate-manage right to silently delete various groups' metadata.	2021-07-02	4	CVE-2021-36129 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalRenameRequest page is vulnerable to infinite loops and denial of service attacks when a user's current username is beyond an arbitrary maximum configuration value (MaxNameChars).	2021-07-02	5	CVE-2021-36125 MISC MISC
mediawiki -- mediawiki	An issue was discovered in the CentralAuth extension in MediaWiki through 1.36. The Special:GlobalUserRights page provided search results which, for a suppressed MediaWiki user, were different than for any other user, thus easily disclosing suppressed accounts (which are supposed to be completely hidden).	2021-07-02	4	CVE-2021-36127 MISC MISC
mediawiki -- mediawiki	In MediaWiki before 1.31.15, 1.32.x through 1.35.x before 1.35.3, and 1.36.x before 1.36.1, bots have certain unintended API access. When a bot account has a "sitewide block" applied, it is able to still "purge" pages through the MediaWiki Action API (which a "sitewide block" should have prevented).	2021-07-02	5	CVE-2021-35197 CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in the FileImporter extension in MediaWiki through 1.36. For certain relaxed configurations of the $wgFileImporterRequiredRight variable, it might not validate all appropriate user rights, thus allowing a user with insufficient rights to perform operations (specifically file uploads) that they should not be allowed to perform.	2021-07-02	6	CVE-2021-36132 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mikrotik -- routeros	Mikrotik RouterOs before 6.47 (stable tree) suffers from an assertion failure vulnerability in the /nova/bin/user process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.	2021-07-07	4	CVE-2020-20225 MISC FULLDISC
mikrotik -- routeros	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/graphing process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-07-07	4	CVE-2020-20216 MISC MISC
mikrotik -- routeros	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/diskd process. An authenticated remote attacker can cause a Denial of Service due to invalid memory access.	2021-07-07	4	CVE-2020-20215 MISC MISC
mikrotik -- routeros	Mikrotik RouterOs 6.44.5 (long-term tree) suffers from an stack exhaustion vulnerability in the /nova/bin/net process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	2021-07-07	4	CVE-2020-20213 MISC MISC
mikrotik -- routeros	Mikrotik RouterOs 6.44.5 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/console process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-07-07	4	CVE-2020-20212 MISC MISC
mikrotik -- routeros	Mikrotik RouterOs 6.44.5 (long-term tree) suffers from an assertion failure vulnerability in the /nova/bin/console process. An authenticated remote attacker can cause a Denial of Service due to an assertion failure via a crafted packet.	2021-07-07	4	CVE-2020-20211 MISC MISC
misp -- misp	app/View/SharingGroups/view.ctp in MISP before 2.4.146 allows stored XSS in the sharing groups view.	2021-07-07	4.3	CVE-2021-36212 MISC MISC
mooveagency -- import_xml_and_rss_feeds	Server-side request forgery (SSRF) in the Import XML and RSS Feeds (import-xml-feed) plugin 2.0.1 for WordPress via the data parameter in a moove_read_xml action.	2021-07-07	6.4	CVE-2020-24148 MISC MISC
ninja -- video_downloader_for_tiktok	Directory traversal in the Video Downloader for TikTok (aka downloader-tiktok) plugin 1.3 for WordPress lets an attacker get access to files that are stored outside the web root folder via the njt-tk-download-video parameter.	2021-07-07	5	CVE-2020-24143 MISC
ninjarmm -- ninjarmm	The Agent in NinjaRMM 5.0.909 has Incorrect Access Control.	2021-07-07	4.6	CVE-2021-26273 MISC MISC MISC
nsa -- emissary	Emissary is a P2P-based, data-driven workflow engine. Emissary version 6.4.0 is vulnerable to Server-Side Request Forgery (SSRF). In particular, the `RegisterPeerAction` endpoint and the `AddChildDirectoryAction` endpoint are vulnerable to SSRF. This vulnerability may lead to credential leaks. Emissary version 7.0 contains a patch. As a workaround, disable network access to Emissary from untrusted sources.	2021-07-02	6.5	CVE-2021-32639 CONFIRM MISC MISC
openvpn -- connect	OpenVPN Connect 3.2.0 through 3.3.0 allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (OpenVPNConnect.exe).	2021-07-02	4.4	CVE-2021-3613 MISC
openvpn -- openvpn	OpenVPN before version 2.5.3 on Windows allows local users to load arbitrary dynamic loadable libraries via an OpenSSL configuration file if present, which allows the user to run arbitrary code with the same privilege level as the main OpenVPN process (openvpn.exe).	2021-07-02	4.4	CVE-2021-3606 MISC MISC
pexip -- pexip_infinity	Pexip Infinity 22.x through 24.x before 24.2 has Improper Input Validation for call setup. An unauthenticated remote attacker can trigger a software abort (temporary loss of service).	2021-07-07	5	CVE-2020-25868 MISC CONFIRM
pexip -- pexip_infinity	Pexip Infinity 25.x before 25.4 has Improper Input Validation, and thus an unauthenticated remote attacker can cause a denial of service via the administrative web interface.	2021-07-07	5	CVE-2021-31925 MISC CONFIRM
php-fusion -- php-fusion	An issue exists in PHP-Fusion 9.03.50 where session cookies are not deleted once a user logs out, allowing for an attacker to perform a session replay attack and impersonate the victim user.	2021-07-02	5.5	CVE-2020-23178 MISC
php-fusion -- php-fusion	The component /php-fusion/infusions/shoutbox_panel/shoutbox_archive.php in PHP-Fusion 9.03.60 allows attackers to redirect victim users to malicious websites via a crafted payload entered into the Shoutbox message panel.	2021-07-02	4.9	CVE-2020-23182 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
profilepress -- wp-user-avatar	A vulnerability in the user profile update component found in the ~/src/Classes/EditUserProfile.php file of the ProfilePress WordPress plugin made it possible for users to escalate their privileges to that of an administrator while editing their profile. This issue affects versions 3.0.0 - 3.1.3. .	2021-07-07	6.5	CVE-2021-34622 MISC
pywin32_project -- pywin32	An integer overflow exists in pywin32 prior to version b301 when adding an access control entry (ACE) to an access control list (ACL) that would cause the size to be greater than 65535 bytes. An attacker who successfully exploited this vulnerability could crash the vulnerable process.	2021-07-06	4	CVE-2021-32559 MISC MISC
qsan -- sanos	Improper restriction of excessive authentication attempts vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to discover users' credentials and obtain access via a brute force attack.	2021-07-07	5	CVE-2021-32522 CONFIRM
qsan -- sanos	Use of password hash with insufficient computational effort vulnerability in QSAN Storage Manager, XEVO, SANOS allows remote attackers to recover the plain-text password by brute-forcing the MD5 hash.	2021-07-07	5	CVE-2021-32519 CONFIRM
qsan -- storage_manager	Improper access control vulnerability in FirmwareUpgrade in QSAN Storage Manager allows remote attackers to reboot and discontinue the device.	2021-07-07	5	CVE-2021-32514 CONFIRM
qsan -- storage_manager	Path traversal vulnerability in QSAN Storage Manager allows remote unauthenticated attackers to download arbitrary files thru injecting file path in download function.	2021-07-07	5	CVE-2021-32527 CONFIRM
qsan -- storage_manager	Observable behavioral discrepancy vulnerability in QSAN Storage Manager allows remote attackers to obtain the system information without permissions.	2021-07-07	5	CVE-2021-32528 CONFIRM
qsan -- storage_manager	Command injection vulnerability in QSAN Storage Manager allows remote privileged users to execute arbitrary commands.	2021-07-07	6.5	CVE-2021-32524 CONFIRM
qsan -- storage_manager	A vulnerability in share_link in QSAN Storage Manager allows remote attackers to create a symbolic link then access arbitrary files.	2021-07-07	5	CVE-2021-32518 CONFIRM
qsan -- storage_manager	Absolute Path Traversal vulnerability in FileDownload in QSAN Storage Manager allows remote authenticated attackers download arbitrary files via the Url path parameter.	2021-07-07	4	CVE-2021-32507 CONFIRM
qsan -- storage_manager	Improper access control vulnerability in share_link in QSAN Storage Manager allows remote attackers to download arbitrary files using particular parameter in download function.	2021-07-07	5	CVE-2021-32517 CONFIRM
qsan -- storage_manager	Absolute Path Traversal vulnerability in GetImage in QSAN Storage Manager allows remote authenticated attackers download arbitrary files via the Url path parameter.	2021-07-07	4	CVE-2021-32506 CONFIRM
qsan -- storage_manager	Absolute Path Traversal vulnerability in FileStreaming in QSAN Storage Manager allows remote authenticated attackers access arbitrary files by injecting the Symbolic Link following the Url path parameter.	2021-07-07	4	CVE-2021-32508 CONFIRM
qsan -- storage_manager	Absolute Path Traversal vulnerability in FileviewDoc in QSAN Storage Manager allows remote authenticated attackers access arbitrary files by injecting the Symbolic Link following the Url path parameter.	2021-07-07	4	CVE-2021-32509 CONFIRM
qsan -- storage_manager	QSAN Storage Manager through directory listing vulnerability in antivirus function allows remote authenticated attackers to list arbitrary directories by injecting file path parameter.	2021-07-07	4	CVE-2021-32510 CONFIRM
qsan -- storage_manager	QSAN Storage Manager through directory listing vulnerability in ViewBroserList allows remote authenticated attackers to list arbitrary directories via the file path parameter.	2021-07-07	4	CVE-2021-32511 CONFIRM
qsan -- storage_manager	Incorrect permission assignment for critical resource vulnerability in QSAN Storage Manager allows authenticated remote attackers to access arbitrary password files.	2021-07-07	4	CVE-2021-32526 CONFIRM
qsan -- storage_manager	Path traversal vulnerability in share_link in QSAN Storage Manager allows remote attackers to download arbitrary files.	2021-07-07	5	CVE-2021-32516 CONFIRM
qsan -- storage_manager	Directory listing vulnerability in share_link in QSAN Storage Manager allows attackers to list arbitrary directories and further access credential information.	2021-07-07	5	CVE-2021-32515 CONFIRM
qsan -- storage_manager	Improper authorization vulnerability in QSAN Storage Manager allows remote privileged users to bypass the access control and execute arbitrary commands.	2021-07-07	6.5	CVE-2021-32523 CONFIRM
qsan -- xevo	Path traversal vulnerability in back-end analysis function in QSAN XEVO allows remote attackers to download arbitrary files without permissions.	2021-07-07	5	CVE-2021-32532 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rocket.chat -- rocket.chat	The Rocket.Chat desktop application 2.17.11 opens external links without user interaction.	2021-07-05	5	CVE-2020-26763 MISC
sitasoftware -- azurcms	A SQL injection vulnerability in azurWebEngine in Sita AzurCMS through 1.2.3.12 allows an authenticated attacker to execute arbitrary SQL commands via the id parameter to mesdocs.ajax.php in azurWebEngine/eShop. By default, the query is executed as DBA.	2021-07-02	6.5	CVE-2021-27950 MISC MISC MISC MISC
smashing_project -- smashing	Smashing 1.3.4 is vulnerable to Cross Site Scripting (XSS). A URL for a widget can be crafted and used to execute JavaScript on the victim's computer. The JavaScript code can then steal data available in the session/cookies depending on the user environment (e.g. if re-using internal URL's for deploying, or cookies that are very permissive) private information may be retrieved by the attacker.	2021-07-06	4.3	CVE-2021-35440 MISC MISC MISC
tcl -- tcl	** DISPUTED ** In Tcl 8.6.11, a format string vulnerability in nmakehlp.c might allow code execution via a crated file. NOTE: multiple third parties dispute the significance of this finding.	2021-07-05	6.8	CVE-2021-35331 MISC MISC MISC MISC
teradici -- pcoip_management_console	In Teradici PCoIP Management Console-Enterprise 20.07.0, an unauthenticated user can inject arbitrary text into user browser via the Web application.	2021-07-07	4.3	CVE-2021-35451 MISC MISC
tielabs -- jannah	The Jannah WordPress theme before 5.4.5 did not properly sanitize the 'query' POST parameter in its tie_ajax_search AJAX action, leading to a Reflected Cross-site Scripting (XSS) vulnerability.	2021-07-06	4.3	CVE-2021-24407 CONFIRM
webkitgtk -- webkitgtk	A use-after-free vulnerability exists in the way certain events are processed for ImageLoader objects of Webkit WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. In order to trigger the vulnerability, a victim must be tricked into visiting a malicious webpage.	2021-07-07	6.8	CVE-2021-21775 MISC
wp-currency -- wordpress_currency_switcher	Cross-site request forgery (CSRF) vulnerability in WPCS - WordPress Currency Switcher 1.1.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-07	6.8	CVE-2021-20780 MISC MISC MISC
wp-downloadmanager_project -- wp-download_manager	Server-side request forgery in the WP-DownloadManager plugin 1.68.4 for WordPress lets an attacker send crafted requests from the back-end server of a vulnerable web application via the file_remote parameter to download-add.php. It can help identify open ports, local network hosts and execute command on services	2021-07-07	5	CVE-2020-24141 MISC
wp-upload-restriction_project -- wp-upload-restriction	A vulnerability in the deleteCustomType function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to delete custom extensions added by administrators. This issue affects versions 2.2.3 and prior.	2021-07-07	4	CVE-2021-34626 MISC
zimbra -- collaboration	An open redirect vulnerability exists in the /preauth Servlet in Zimbra Collaboration Suite through 9.0. To exploit the vulnerability, an attacker would need to have obtained a valid zimbra auth token or a valid preauth token. Once the token is obtained, an attacker could redirect a user to any URL via isredirect=1&redirectURL= in conjunction with the token data (e.g., a valid authtoken= value).	2021-07-02	5.8	CVE-2021-34807 MISC MISC MISC MISC
zimbra -- collaboration	An issue was discovered in ProxyServlet.java in the /proxy servlet in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.x before 9.0.0 Patch 16. The value of the X-Host header overwrites the value of the Host header in proxied requests. The value of X-Host header is not checked against the whitelist of hosts Zimbra is allowed to proxy to (the zimbraProxyAllowedDomains setting).	2021-07-02	5.8	CVE-2021-35209 MISC MISC MISC MISC
zimbra -- collaboration	An issue was discovered in Zimbra Collaboration Suite 8.8 before 8.8.15 Patch 23 and 9.0 before 9.0.0 Patch 16. An XSS vulnerability exists in the login component of Zimbra Web Client, in which an attacker can execute arbitrary JavaScript by adding executable JavaScript to the loginErrorCode parameter of the login url.	2021-07-02	4.3	CVE-2021-35207 MISC MISC MISC MISC
zohocorp -- manageengine_adselfservice_plus	Zoho ManageEngine ADSelfService Plus before 6104, in rare situations, allows attackers to obtain sensitive information about the password-sync database application.	2021-07-02	4.3	CVE-2021-31874 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Search Text" field under the "Admin Search" module.	2021-07-02	3.5	CVE-2020-36412 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Create a new Design" parameter under the "Designs" module.	2021-07-02	3.5	CVE-2020-36416 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "URL (slug)" or "Extra" fields under the "Add Article" feature.	2021-07-02	3.5	CVE-2020-36414 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Exclude these IP addresses from the "Site Down" status" parameter under the "Maintenance Mode" module.	2021-07-02	3.5	CVE-2020-36413 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Path for the {page_image} tag:" or "Path for thumbnail field:" parameters under the "Content Editing Settings" module.	2021-07-02	3.5	CVE-2020-36411 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Email address to receive notification of news submission" parameter under the "Options" module.	2021-07-02	3.5	CVE-2020-36410 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add Category" parameter under the "Categories" module.	2021-07-02	3.5	CVE-2020-36409 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Add Shortcut" parameter under the "Manage Shortcuts" module.	2021-07-02	3.5	CVE-2020-36408 MISC
cmsmadesimple -- cms_made_simple	A stored cross scripting (XSS) vulnerability in CMS Made Simple 2.2.14 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Create a new Stylesheet" parameter under the "Stylesheets" module.	2021-07-02	3.5	CVE-2020-36415 MISC
deliciousbrains -- wp_offload_ses_lite	The WP Offload SES Lite WordPress plugin before 1.4.5 did not escape some of the fields in the Activity page of the admin dashboard, such as the email's id, subject and recipient, which could lead to Stored Cross-Site Scripting issues when an attacker can control any of these fields, like the subject when filling a contact form for example. The XSS will be executed in the context of a logged in admin viewing the Activity tab of the plugin.	2021-07-06	3.5	CVE-2021-24494 CONFIRM
e4j -- vikrentcar_car_rental_management_system	In the VikRentCar Car Rental Management System WordPress plugin before 1.1.7, there is a custom filed option by which we can manage all the fields that the users will have to fill in before saving the order. However, the field name is not sanitised or escaped before being output back in the page, leading to a stored Cross-Site Scripting issue. There is also no CSRF check done before saving the setting, allowing attackers to make a logged in admin set arbitrary Custom Fields, including one with XSS payload in it.	2021-07-06	3.5	CVE-2021-24388 CONFIRM
getkirby -- kirby	Kirby is a content management system. In Kirby CMS versions 3.5.5 and 3.5.6, the Panel's `ListItem` component (used in the pages and files section for example) displayed HTML in page titles as it is. This could be used for cross-site scripting (XSS) attacks. Malicious authenticated Panel users can escalate their privileges if they get access to the Panel session of an admin user. Visitors without Panel access can use the attack vector if the site allows changing site data from a frontend form. Kirby 3.5.7 patches the vulnerability. As a partial workaround, site administrators can protect against attacks from visitors without Panel access by validating or sanitizing provided data from the frontend form.	2021-07-02	3.5	CVE-2021-32735 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gitlab -- gitlab	HTML injection was possible via the full name field before versions 13.11.6, 13.12.6, and 14.0.2 in GitLab CE	2021-07-06	3.5	CVE-2021-22232 CONFIRM MISC MISC
gitlab -- gitlab	Insufficient input sanitization in markdown in GitLab version 13.11 and up allows an attacker to exploit a stored cross-site scripting vulnerability via a specially-crafted markdown	2021-07-07	3.5	CVE-2021-22225 MISC CONFIRM
irislink -- irisnext	Multiple stored XSS vulnerabilities in IrisNext Edition 9.5.16, which allows an authenticated (or compromised) user to inject malicious JavaScript in folder/file name within the application in order to grab other users' sessions or execute malicious code in their browsers (1-click RCE).	2021-07-06	3.5	CVE-2021-27930 MISC MISC
issabel -- pbx	A stored cross site scripting (XSS) vulnerability in index.php?menu=billing_rates of Issabel PBX version 4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Name" or "Prefix" fields under the "Create New Rate" module.	2021-07-06	3.5	CVE-2021-34190 MISC MISC
kubiq -- wp_svg_images	The WP SVG images WordPress plugin before 3.4 did not sanitise the SVG files uploaded, which could allow low privilege users such as author+ to upload a malicious SVG and then perform XSS attacks by inducing another user to access the file directly. In v3.4, the plugin restricted such upload to editors and admin, with an option to also allow author to do so. The description of the plugin has also been updated with a security warning as upload of such content is intended.	2021-07-06	3.5	CVE-2021-24386 CONFIRM
lavalite -- lavalite	A stored cross site scripting (XSS) vulnerability in the /admin/user/team component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	2021-07-02	3.5	CVE-2020-36395 MISC
lavalite -- lavalite	A stored cross site scripting (XSS) vulnerability in the /admin/contact/contact component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	2021-07-02	3.5	CVE-2020-36397 MISC
lavalite -- lavalite	A stored cross site scripting (XSS) vulnerability in the /admin/roles/role component of LavaLite 5.8.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "New" parameter.	2021-07-02	3.5	CVE-2020-36396 MISC
mediawiki -- mediawiki	An XSS issue was discovered in the SocialProfile extension in MediaWiki through 1.36. Within several gift-related special pages, a privileged user with the awardmanage right could inject arbitrary HTML and JavaScript within various gift-related data fields. The attack could easily propagate across many pages for many users.	2021-07-02	3.5	CVE-2021-36130 MISC MISC
mediawiki -- mediawiki	An XSS issue was discovered in the SportsTeams extension in MediaWiki through 1.36. Within several special pages, a privileged user could inject arbitrary HTML and JavaScript within various data fields. The attack could easily propagate across many pages for many users.	2021-07-02	3.5	CVE-2021-36131 MISC MISC
monstra -- monstra_cms	Cross Site Scripting vulnerabilty in Monstra CMS 3.0.4 via the page feature in admin/index.php.	2021-07-06	3.5	CVE-2020-23697 MISC
ninjarmm -- ninjarmm	The Agent in NinjaRMM 5.0.909 has Insecure Permissions.	2021-07-07	3.6	CVE-2021-26274 MISC MISC MISC
openexr -- openexr	There's a flaw in OpenEXR's ImfDeepScanLineInputFile functionality in versions prior to 3.0.5. An attacker who is able to submit a crafted file to an application linked with OpenEXR could cause an out-of-bounds read. The greatest risk from this flaw is to application availability.	2021-07-06	2.1	CVE-2021-3598 MISC
php-fusion -- php-fusion	A stored cross site scripting (XSS) vulnerability in /administration/settings_registration.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Registration" field.	2021-07-02	3.5	CVE-2020-23184 MISC
php-fusion -- php-fusion	A stored cross site scripting (XSS) vulnerability in /administration/setting_security.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-07-02	3.5	CVE-2020-23185 MISC
php-fusion -- php-fusion	A reflected cross site scripting (XSS) vulnerability in /administration/theme.php of PHP-Fusion 9.03.60 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Manage Theme" field.	2021-07-02	3.5	CVE-2020-23181 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
php-fusion -- php-fusion	A stored cross site scripting (XSS) vulnerability in administration/settings_main.php of PHP-Fusion 9.03.50 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Site footer" field.	2021-07-02	3.5	CVE-2020-23179 MISC
phplist -- phplist	Cross Site Scripting (XSS) vulnerability in phpList 3.5.3 via the login name field in Manage Administrators when adding a new admin.	2021-07-06	3.5	CVE-2020-22251 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the "rule1" parameter under the "Bounce Rules" module.	2021-07-02	3.5	CVE-2020-36399 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the "Campaign" field under the "Send a campaign" module.	2021-07-02	3.5	CVE-2020-36398 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in the "Import Subscribers" feature in phplist 3.5.4 and below allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-07-02	3.5	CVE-2020-23194 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in phplist 3.5.4 and below allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload in the "admin" parameter under the "Manage administrators" module.	2021-07-02	3.5	CVE-2020-23192 MISC
phplist -- phplist	A stored cross site scripting (XSS) vulnerability in the "Import emails" module in phplist 3.5.4 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload.	2021-07-02	3.5	CVE-2020-23190 MISC
sulu -- sulu	Sulu is an open-source PHP content management system based on the Symfony framework. In versions of Sulu prior to 1.6.41, it is possible for a logged in admin user to add a script injection (cross-site-scripting) in the collection title. The problem is patched in version 1.6.41. As a workaround, one may manually patch the affected JavaScript files in lieu of updating.	2021-07-02	3.5	CVE-2021-32737 CONFIRM MISC
wp-upload-restriction_project -- wp-upload-restriction	A vulnerability in the saveCustomType function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to inject arbitrary web scripts. This issue affects versions 2.2.3 and prior.	2021-07-07	3.5	CVE-2021-34625 MISC
wp-upload-restriction_project -- wp-upload-restriction	A vulnerability in the getSelectedMimeTypesByRole function of the WP Upload Restriction WordPress plugin allows low-level authenticated users to view custom extensions added by administrators. This issue affects versions 2.2.3 and prior.	2021-07-07	3.5	CVE-2021-34627 MISC
zimbra -- collaboration	An issue was discovered in ZmMailMsgView.js in the Calendar Invite component in Zimbra Collaboration Suite 8.8.x before 8.8.15 Patch 23. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.	2021-07-02	3.5	CVE-2021-35208 MISC MISC MISC MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a-stage.inc -- sct-40cm01sr_and_at-40cm01sr	Improper authentication vulnerability in SCT-40CM01SR and AT-40CM01SR allows an attacker to bypass access restriction and execute an arbitrary command via telnet.	2021-07-07	not yet calculated	CVE-2021-20776 MISC
accusoft -- imagegear	An out-of-bounds write vulnerability exists in the TIF bits_per_sample processing functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	2021-07-08	not yet calculated	CVE-2021-21794 MISC
accusoft -- imagegear	A stack-based buffer overflow vulnerability exists in the PDF process_fontname functionality of Accusoft ImageGear 19.9. A specially crafted malformed file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	2021-07-08	not yet calculated	CVE-2021-21821 MISC
accusoft -- imagegear	An out-of-bounds write vulnerability exists in the JPG sof_nb_comp header processing functionality of Accusoft ImageGear 19.8 and 19.9. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	2021-07-08	not yet calculated	CVE-2021-21793 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arcgis -- server_manager	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	2021-07-10	not yet calculated	CVE-2021-29107 CONFIRM
arcgis -- server_manager	A reflected Cross Site Scripting (XXS) vulnerability in ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	2021-07-10	not yet calculated	CVE-2021-29106 CONFIRM
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34616 MISC
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34614 MISC
aruba -- clearpass_policy_manager	A remote denial of service (DoS) vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-29152 MISC
aruba -- clearpass_policy_manager	A remote authentication bypass vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-29151 MISC
aruba -- clearpass_policy_manager	A remote insecure deserialization vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-29150 MISC
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34613 MISC
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34612 MISC
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34611 MISC
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34610 MISC
aruba -- clearpass_policy_manager	A remote arbitrary command execution vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34615 MISC
aruba -- clearpass_policy_manager	A remote SQL injection vulnerability was discovered in Aruba ClearPass Policy Manager version(s): Prior to 6.10.0, 6.9.6 and 6.8.9. Aruba has released updates to ClearPass Policy Manager that address this security vulnerability.	2021-07-08	not yet calculated	CVE-2021-34609 MISC
autodesk -- autodesk	A maliciously crafted TIFF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read and write beyond allocated boundaries when parsing the TIFF file. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	not yet calculated	CVE-2021-27039 MISC
autodesk -- autodesk	A maliciously crafted PNG, PDF or DWF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be used to attempt to free an object that has already been freed while parsing them. This vulnerability can be exploited by remote attackers to execute arbitrary code.	2021-07-09	not yet calculated	CVE-2021-27037 MISC
autodesk -- autodesk	A heap-based buffer overflow could occur while parsing PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	not yet calculated	CVE-2021-27034 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- autodesk	A Type Confusion vulnerability in Autodesk 2018, 2017, 2013, 2012, 2011 can occur when processing a maliciously crafted PDF file. An attacker can leverage this to execute arbitrary code.	2021-07-09	not yet calculated	CVE-2021-27038 MISC
autodesk -- autodesk	A maliciously crafted PDF, PICT or TIFF file can be used to write beyond the allocated buffer while parsing PDF, PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	not yet calculated	CVE-2021-27036 MISC
autodesk -- autodesk	A maliciously crafted TIFF, PDF, PICT or DWF files in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read beyond allocated boundaries when parsing the TIFF, PDF, PICT or DWF files. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	not yet calculated	CVE-2021-27035 MISC
autodesk -- design_review	A Double Free vulnerability allows remote attackers to execute arbitrary code on PDF files within affected installations of Autodesk Design Review. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.	2021-07-09	not yet calculated	CVE-2021-27033 MISC
baigo -- cms	A cross site scripting vulnerability in baigo CMS v4.0-beta-1 allows attackers to execute arbitrary web scripts or HTML via the form parameter post to /public/console/profile/info-submit/.	2021-07-08	not yet calculated	CVE-2020-20584 MISC MISC MISC MISC
blackcat_cms -- blackcat_cms	A stored cross site scripting (XSS) vulnerability in the 'Admin-Tools' feature of BlackCat CMS 1.3.6 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payloads entered into the 'Output Filters' and 'Droplets' modules.	2021-07-09	not yet calculated	CVE-2020-25878 MISC MISC
blackcat_cms -- blackcat_cms	A stored cross site scripting (XSS) vulnerability in the 'Add Page' feature of BlackCat CMS 1.3.6 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	2021-07-09	not yet calculated	CVE-2020-25877 MISC MISC
cisco -- adaptive_security_device_manager	A vulnerability in the Cisco Adaptive Security Device Manager (ASDM) Launcher could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating system. This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code. A successful exploit could allow the attacker to execute arbitrary code on the user's operating system with the level of privileges assigned to the ASDM Launcher. A successful exploit may require the attacker to perform a social engineering attack to persuade the user to initiate communication from the Launcher to the ASDM.	2021-07-08	not yet calculated	CVE-2021-1585 CISCO
cisco -- asyncos	A vulnerability in the configuration management of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to perform command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied XML input for the web interface. An attacker could exploit this vulnerability by uploading crafted XML configuration files that contain scripting code to a vulnerable device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. An attacker would need a valid user account with the rights to upload configuration files to exploit this vulnerability.	2021-07-08	not yet calculated	CVE-2021-1359 CISCO
cisco -- broadworks_application_server	A vulnerability in the XSI-Actions interface of Cisco BroadWorks Application Server could allow an authenticated, remote attacker to access sensitive information on an affected system. This vulnerability is due to improper input validation and authorization of specific commands that a user can execute within the XSI-Actions interface. An attacker could exploit this vulnerability by authenticating to an affected device and issuing a specific set of commands. A successful exploit could allow the attacker to join a Call Center instance and have calls that they do not have permissions to access distributed to them from the Call Center queue. At the time of publication, Cisco had not released updates that address this vulnerability for Cisco BroadWorks Application Server. However, firmware patches are available.	2021-07-08	not yet calculated	CVE-2021-1562 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- business_process_automation	Multiple vulnerabilities in the web-based management interface of Cisco Business Process Automation (BPA) could allow an authenticated, remote attacker to elevate privileges to Administrator. These vulnerabilities are due to improper authorization enforcement for specific features and for access to log files that contain confidential information. An attacker could exploit these vulnerabilities either by submitting crafted HTTP messages to an affected system and performing unauthorized actions with the privileges of an administrator, or by retrieving sensitive data from the logs and using it to impersonate a legitimate privileged user. A successful exploit could allow the attacker to elevate privileges to Administrator.	2021-07-08	not yet calculated	CVE-2021-1574 CISCO
cisco -- business_process_automation	Multiple vulnerabilities in the web-based management interface of Cisco Business Process Automation (BPA) could allow an authenticated, remote attacker to elevate privileges to Administrator. These vulnerabilities are due to improper authorization enforcement for specific features and for access to log files that contain confidential information. An attacker could exploit these vulnerabilities either by submitting crafted HTTP messages to an affected system and performing unauthorized actions with the privileges of an administrator, or by retrieving sensitive data from the logs and using it to impersonate a legitimate privileged user. A successful exploit could allow the attacker to elevate privileges to Administrator.	2021-07-08	not yet calculated	CVE-2021-1576 CISCO
cisco -- identity_services_engine	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	2021-07-08	not yet calculated	CVE-2021-1607 CISCO
cisco -- identity_services_engine	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	2021-07-08	not yet calculated	CVE-2021-1606 CISCO
cisco -- identity_services_engine	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	2021-07-08	not yet calculated	CVE-2021-1605 CISCO
cisco -- identity_services_engine	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	2021-07-08	not yet calculated	CVE-2021-1604 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- identity_services_engine	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user. These vulnerabilities exist because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker would need valid administrative credentials.	2021-07-08	not yet calculated	CVE-2021-1603 CISCO
cisco -- video_surveillance_7000_ip_cameras	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2021-07-08	not yet calculated	CVE-2021-1598 CISCO
cisco -- video_surveillance_7000_series_ip_cameras	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2021-07-08	not yet calculated	CVE-2021-1597 CISCO
cisco -- video_surveillance_7000_series_ip_cameras	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2021-07-08	not yet calculated	CVE-2021-1595 CISCO
cisco -- video_surveillance_7000_series_ip_cameras	Multiple vulnerabilities in the Link Layer Discovery Protocol (LLDP) implementation for Cisco Video Surveillance 7000 Series IP Cameras could allow an unauthenticated, adjacent attacker to cause a memory leak, which could lead to a denial of service (DoS) condition on an affected device. These vulnerabilities are due to incorrect processing of certain LLDP packets at ingress time. An attacker could exploit these vulnerabilities by sending crafted LLDP packets to an affected device. A successful exploit could allow the attacker to cause the affected device to continuously consume memory, which could cause the device to crash and reload, resulting in a DoS condition. Note: LLDP is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2021-07-08	not yet calculated	CVE-2021-1596 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- virtualized_voice_browser	A vulnerability in the web-based management interface of Cisco Virtualized Voice Browser could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2021-07-08	not yet calculated	CVE-2021-1575 CISCO
codoforum -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Manage Users' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Username' parameter.	2021-07-09	not yet calculated	CVE-2020-25879 MISC MISC
codoforum -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Smileys' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Smiley Code' parameter.	2021-07-09	not yet calculated	CVE-2020-25875 MISC MISC
codoforum -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Pages' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Page Title' parameter.	2021-07-09	not yet calculated	CVE-2020-25876 MISC MISC
csz-cms -- csz-cms	A cross site scripting vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New Pages' field under the 'Pages Content' module.	2021-07-09	not yet calculated	CVE-2020-25391 MISC
csz-cms -- csz-cms	A cross site scripting (XSS) vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New Article' field under the 'Article' plugin.	2021-07-09	not yet calculated	CVE-2020-25392 MISC
dotAdmin/#/c/containers -- dotAdmin/#/c/containers	A stored cross site scripting (XSS) vulnerability in dotAdmin/#/c/c_Images of dotCMS 21.05.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' and 'Filename' parameters.	2021-07-09	not yet calculated	CVE-2021-35358 MISC
dotAdmin/#/c/containers -- dotAdmin/#/c/containers	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/containers of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	2021-07-09	not yet calculated	CVE-2021-35360 MISC
dotAdmin/#/c/containers -- dotAdmin/#/c/containers	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/links of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	2021-07-09	not yet calculated	CVE-2021-35361 MISC
ecplise -- tinydtls	Eclipse TinyDTLS through 0.9-rc1 relies on the rand function in the C library, which makes it easier for remote attackers to compute the master key and then decrypt DTLS traffic.	2021-07-08	not yet calculated	CVE-2021-34430 CONFIRM
edgex -- foundry	EdgeX Foundry is an open source project for building a common open framework for internet-of-things edge computing. A vulnerability exists in the Edinburgh, Fuji, Geneva, and Hanoi versions of the software. When the EdgeX API gateway is configured for OAuth2 authentication and a proxy user is created, the client_id and client_secret required to obtain an OAuth2 authentication token are set to the username of the proxy user. A remote network attacker can then perform a dictionary-based password attack on the OAuth2 token endpoint of the API gateway to obtain an OAuth2 authentication token and use that token to make authenticated calls to EdgeX microservices from an untrusted network. OAuth2 is the default authentication method in EdgeX Edinburgh release. The default authentication method was changed to JWT in Fuji and later releases. Users should upgrade to the EdgeX Ireland release to obtain the fix. The OAuth2 authentication method is disabled in Ireland release. If unable to upgrade and OAuth2 authentication is required, users should create OAuth2 users directly using the Kong admin API and forgo the use of the `security-proxy-setup` tool to create OAuth2 users.	2021-07-09	not yet calculated	CVE-2021-32753 MISC CONFIRM
elecom -- multiple_products	WRC-1167FS-W, WRC-1167FS-B, and WRC-1167FSA all versions allow an unauthenticated network-adjacent attacker to obtain sensitive information via unspecified vectors.	2021-07-07	not yet calculated	CVE-2021-20738 MISC MISC
emissary-ingress -- emissary-ingress	Emissary-Ingress (formerly Ambassador API Gateway) through 1.13.9 allows attackers to bypass client certificate requirements (i.e., mTLS cert_required) on backend upstreams when more than one TLSContext is defined and at least one configuration exists that does not require client certificate authentication. The attacker must send an SNI specifying an unprotected backend and an HTTP Host header specifying a protected backend.	2021-07-09	not yet calculated	CVE-2021-36371 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ether_logs -- ether_logs	Ether Logs is a package that allows one to check one's logs in the Craft 3 utilities section. A vulnerability was found in versions prior to 3.0.4 that allowed authenticated admin users to access any file on the server. The vulnerability has been fixed in version 3.0.4. As a workaround, one may disable the plugin if untrustworthy sources have admin access.	2021-07-09	not yet calculated	CVE-2021-32752 CONFIRM MISC
fork -- fork	Arbitrary file upload vulnerability in Fork CMS 5.9.2 allows attackers to create or replace arbitrary files in the /themes directory via a crafted zip file uploaded to the Themes panel.	2021-07-07	not yet calculated	CVE-2021-28931 MISC MISC
fortinet -- fortiap	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments.	2021-07-09	not yet calculated	CVE-2021-26106 CONFIRM
fortinet -- fortimail	Multiple improper neutralization of special elements of SQL commands vulnerabilities in FortiMail before 6.4.4 may allow a non-authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	not yet calculated	CVE-2021-24007 CONFIRM
fortinet -- fortimail	A missing cryptographic step in the implementation of the hash digest algorithm in FortiMail 6.4.0 through 6.4.4, and 6.2.0 through 6.2.7 may allow an unauthenticated attacker to tamper with signed URLs by appending further data which allows bypass of signature verification.	2021-07-09	not yet calculated	CVE-2021-24020 CONFIRM
fortinet -- fortimail	A missing cryptographic step in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an unauthenticated attacker who intercepts the encrypted messages to manipulate them in such a way that makes the tampering and the recovery of the plaintexts possible.	2021-07-09	not yet calculated	CVE-2021-26100 CONFIRM
fortinet -- fortimail	Multiple instances of incorrect calculation of buffer size in the Webmail and Administrative interface of FortiMail before 6.4.5 may allow an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	not yet calculated	CVE-2021-22129 CONFIRM
fortinet -- fortisandbox	A concurrent execution using shared resource with improper synchronization ('race condition') in the command shell of FortiSandbox before 3.2.2 may allow an authenticated attacker to bring the system into an unresponsive state via specifically orchestrated sequences of commands.	2021-07-09	not yet calculated	CVE-2020-29014 CONFIRM
foxit -- reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 produce incorrect PDF document signatures because the certificate name, document owner, and signature author are mishandled.	2021-07-09	not yet calculated	CVE-2021-33795 MISC
foxit -- reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write via a crafted /Size key in the Trailer dictionary.	2021-07-09	not yet calculated	CVE-2021-33792 MISC
google -- android	Improper input validation vulnerability in AR Emoji Editor prior to version 4.4.03.5 in Android Q(10.0) and above allows untrusted applications to access arbitrary files with an escalated privilege.	2021-07-08	not yet calculated	CVE-2021-25441 MISC
google -- android	Improper authorization in handler for custom URL scheme vulnerability in GU App for Android versions from 4.8.0 to 5.0.2 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	2021-07-07	not yet calculated	CVE-2021-20777 MISC
hms -- ewon_ecatcher	In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation.	2021-07-09	not yet calculated	CVE-2021-33214 MISC MISC MISC MISC
ibm -- app_connect_enterprise_certified_container	IBM App Connect Enterprise Certified Container 1.0, 1.1, 1.2, and 1.3 could allow a privileged user to obtain sensitive information from internal log files. IBM X-Force ID: 202212.	2021-07-07	not yet calculated	CVE-2021-29759 XF CONFIRM
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 3.0.0.2 and 4.0.0.4 does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.	2021-07-07	not yet calculated	CVE-2021-20474 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 201164.	2021-07-09	not yet calculated	CVE-2021-29730 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 200966.	2021-07-09	not yet calculated	CVE-2021-29712 CONFIRM XF
ibm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 6.2.7.8 , 6.2.7.9, 7.0.3.0, 7.0.4.0, 7.0.5.4, 7.1.0.0, 7.1.1.0, 7.1.1.1, and 7.1.1.2 could allow an authenticated user with certain permissions to initiate an agent upgrade through the CLI interface. IBM X-Force ID: 200965.	2021-07-08	not yet calculated	CVE-2021-29711 CONFIRM XF
iobit -- advanced_systemcare_ultimate	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0dc, the first dword passed in the input buffer is the device port to write to and the word at offset 4 is the value to write via the OUT instruction. The OUT instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users. A local attacker can send a malicious IRP to trigger this vulnerability.	2021-07-07	not yet calculated	CVE-2021-21788 MISC
iobit -- advanced_systemcare_ultimate	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0d8, the first dword passed in the input buffer is the device port to write to and the byte at offset 4 is the value to write via the OUT instruction. The OUT instruction can write one byte to the given I/O device port, potentially leading to escalated privileges of unprivileged users.	2021-07-07	not yet calculated	CVE-2021-21787 MISC
iobit -- advanced_systemcare_ultimate	A privilege escalation vulnerability exists in the way IOBit Advanced SystemCare Ultimate 14.2.0.220 driver handles Privileged I/O write requests. During IOCTL 0x9c40a0e0, the first dword passed in the input buffer is the device port to write to and the dword at offset 4 is the value to write via the OUT instruction. A local attacker can send a malicious IRP to trigger this vulnerability.	2021-07-07	not yet calculated	CVE-2021-21789 MISC
iobit -- advanced_systemcare_ultimate	A privilege escalation vulnerability exists in the IOCTL 0x9c406144 handling of IOBit Advanced SystemCare Ultimate 14.2.0.220. A specially crafted I/O request packet (IRP) can lead to increased privileges. An attacker can send a malicious IRP to trigger this vulnerability.	2021-07-07	not yet calculated	CVE-2021-21786 MISC
kaseya -- vsa	Local file inclusion exists in Kaseya VSA before 9.5.6.	2021-07-09	not yet calculated	CVE-2021-30121 MISC
kaseya -- vsa	Cross Site Scripting (XSS) exists in Kaseya VSA before 9.5.7.	2021-07-09	not yet calculated	CVE-2021-30119 MISC
kaseya -- vsa	Kaseya VSA through 9.5.7 allows attackers to bypass the 2FA requirement.	2021-07-09	not yet calculated	CVE-2021-30120 MISC
kaseya -- vsa	SQL injection exists in Kaseya VSA before 9.5.6.	2021-07-09	not yet calculated	CVE-2021-30117 MISC
kaseya -- vsa	Kaseya VSA before 9.5.5 allows remote code execution.	2021-07-09	not yet calculated	CVE-2021-30118 MISC
kaseya -- vsa	An XML External Entity (XXE) issue exists in Kaseya VSA before 9.5.6.	2021-07-09	not yet calculated	CVE-2021-30201 MISC
keycloak -- keycloak	A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.	2021-07-09	not yet calculated	CVE-2021-3637 MISC
lavalite-cms -- lavalite-cms	Cross Site Scripting (XSS) vulnerability in LavaLite-CMS 5.8.0 via the Menu Links feature.	2021-07-07	not yet calculated	CVE-2020-23700 MISC
libxml2 -- libxlm2	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.	2021-07-09	not yet calculated	CVE-2021-3541 MISC
linux -- linux_kernel	An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-07-09	not yet calculated	CVE-2021-3612 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	kernel/module.c in the Linux kernel before 5.12.14 mishandles Signature Verification, aka CID-0c18f29aae7c. Without CONFIG_MODULE_SIG, verification that a kernel module is signed, for loading via init_module, does not occur for a module.sig_enforce=1 command-line argument.	2021-07-07	not yet calculated	CVE-2021-35039 MISC CONFIRM CONFIRM MLIST
linuxptp -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1.	2021-07-09	not yet calculated	CVE-2021-3570 MISC
linuxptp -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. When ptp4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1.	2021-07-09	not yet calculated	CVE-2021-3571 MISC
ljcms -- r60321	A SQL injection vulnerability in /question.php of LJCMS Version v4.3.R60321 allows attackers to obtain sensitive database information.	2021-07-08	not yet calculated	CVE-2020-20583 MISC
metinfo -- metinfo	A blind SQL injection in /admin/?n=logs&c=index&a=dode of Metinfo 7.0 beta allows attackers to access sensitive database information.	2021-07-08	not yet calculated	CVE-2020-20585 MISC MISC MISC
mikrotik -- routeros	Mikrotik RouterOs before 6.47 (stable tree) suffers from an uncontrolled resource consumption vulnerability in the /nova/bin/route process. An authenticated remote attacker can cause a Denial of Service due to overloading the systems CPU.	2021-07-08	not yet calculated	CVE-2020-20217 MISC MISC
mipcms -- mipcms	A server side request forgery (SSRF) vulnerability in /ApiAdminDomainSettings.php of MipCMS 5.0.1 allows attackers to access sensitive information.	2021-07-08	not yet calculated	CVE-2020-20582 MISC
mozilocms -- mozilocms	A stored cross site scripting (XSS) vulnerability in moziloCMS 2.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Content" parameter.	2021-07-09	not yet calculated	CVE-2020-25394 MISC
octopus -- server	When configuring Octopus Server if it is configured with an external SQL database, on initial configuration the database password is written to the OctopusServer.txt log file in plaintext.	2021-07-08	not yet calculated	CVE-2021-31816 MISC
octopus -- server	When configuring Octopus Server if it is configured with an external SQL database, on initial configuration the database password is written to the OctopusServer.txt log file in plaintext.	2021-07-08	not yet calculated	CVE-2021-31817 MISC
panasonic -- fpwin_pro	Panasonic FPWIN Pro, all Versions 7.5.1.1 and prior, allows an attacker to craft a project file specifying a URI that causes the XML parser to access the URI and embed the contents, which may allow the attacker to disclose information that is accessible in the context of the user executing software.	2021-07-09	not yet calculated	CVE-2021-32972 MISC
pbootcms -- pbootcms	Crossi Site Scripting (XSS) vulnerability in PbootCMS 2.0.3 in admin.php.	2021-07-08	not yet calculated	CVE-2020-20363 MISC MISC MISC
pbootcms -- pbootcms	Incorrect Access Control vulnerability in PbootCMS 2.0.6 via the list parameter in the update function in upgradecontroller.php.	2021-07-09	not yet calculated	CVE-2020-22535 MISC
pbootcms -- pbootcms	Remote Code Execution vulnerability in PbootCMS 2.0.8 in the message board.	2021-07-08	not yet calculated	CVE-2020-23580 MISC
php-fusion -- php-fusion	Cross Site Scripting (XSS) vulnerability in PHP-Fusion 9.03.60 via 'New Shout' in /infusions/shoutbox_panel/shoutbox_admin.php.	2021-07-07	not yet calculated	CVE-2020-23702 MISC MISC
pimcore -- pimcore	This affects the package pimcore/pimcore before 10.0.7. This issue exists due to the absence of check on the storeId parameter in the method collectionsActionGet and groupsActionGet method within the ClassificationstoreController class.	2021-07-09	not yet calculated	CVE-2021-23405 MISC MISC
prusa_research -- prusaslicer	An out-of-bounds write vulnerability exists in the Admesh stl_fix_normal_directions() functionality of Prusa Research PrusaSlicer 2.2.0 and Master (commit 4b040b856). A specially crafted AMF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	2021-07-08	not yet calculated	CVE-2020-28598 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
publiccms -- publiccms	Cross Site Scripting (XSS) vulnerability in PublicCMS 4.0 to get an admin cookie when the Administrator reviews submit case.	2021-07-09	not yet calculated	CVE-2020-21333 MISC
putty -- putty	PuTTY through 0.75 proceeds with establishing an SSH session even if it has never sent a substantive authentication response. This makes it easier for an attacker-controlled SSH server to present a later spoofed authentication prompt (that the attacker can use to capture credential data, and use that data for purposes that are undesired by the client user).	2021-07-09	not yet calculated	CVE-2021-36367 MISC MISC
qnap -- hbs_3	An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3. If exploited, this vulnerability allows attackers to compromise the security of the operating system.QNAP have already fixed this vulnerability in the following versions of HBS 3: QTS 4.3.6: HBS 3 v3.0.210507 and later QTS 4.3.4: HBS 3 v3.0.210506 and later QTS 4.3.3: HBS 3 v3.0.210506 and later	2021-07-08	not yet calculated	CVE-2021-28809 MISC MISC
realtek -- had	Realtek HAD contains a driver crashed vulnerability which allows local side attackers to send a special string to the kernel driver in a user's mode. Due to unexpected commands, the kernel driver will cause the system crashed. A vulnerability in ____COMPONENT____ of Realtek HDA driver allows ____ATTACKER/ATTACK____ to cause ____IMPACT____. This issue affects: Realtek HDA driver 8155 version 9150 and prior versions.	2021-07-07	not yet calculated	CVE-2021-32537 CONFIRM
rockwell_automation -- micrologix_1100	Rockwell Automation MicroLogix 1100, all versions, allows a remote, unauthenticated attacker sending specially crafted commands to cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault whenever the controller is switched to RUN mode.	2021-07-09	not yet calculated	CVE-2021-33012 MISC
ruby -- ruby	Addressable is an alternative implementation to the URI implementation that is part of Ruby's standard library. An uncontrolled resource consumption vulnerability exists after version 2.3.0 through version 2.7.0. Within the URI template implementation in Addressable, a maliciously crafted template may result in uncontrolled resource consumption, leading to denial of service when matched against a URI. In typical usage, templates would not normally be read from untrusted user input, but nonetheless, no previous security advisory for Addressable has cautioned against doing this. Users of the parsing capabilities in Addressable but not the URI template capabilities are unaffected. The vulnerability is patched in version 2.8.0. As a workaround, only create Template objects from trusted sources that have been validated not to produce catastrophic backtracking.	2021-07-06	not yet calculated	CVE-2021-32740 CONFIRM MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Entities List' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	not yet calculated	CVE-2020-35987 MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Global Lists" feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	not yet calculated	CVE-2020-35985 MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Users Access Groups' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	not yet calculated	CVE-2020-35986 MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Users Alerts' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	2021-07-09	not yet calculated	CVE-2020-35984 MISC
rust -- hyper	hyper is an HTTP library for Rust. In versions prior to 0.14.10, hyper's HTTP server and client code had a flaw that could trigger an integer overflow when decoding chunk sizes that are too big. This allows possible data loss, or if combined with an upstream HTTP proxy that allows chunk sizes larger than hyper does, can result in "request smuggling" or "desync attacks." The vulnerability is patched in version 0.14.10. Two possible workarounds exist. One may reject requests manually that contain a `Transfer-Encoding` header or ensure any upstream proxy rejects `Transfer-Encoding` chunk sizes greater than what fits in 64-bit unsigned integers.	2021-07-07	not yet calculated	CVE-2021-32714 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
rust -- hyper	hyper is an HTTP library for rust. hyper's HTTP/1 server code had a flaw that incorrectly parses and accepts requests with a `Content-Length` header with a prefixed plus sign, when it should have been rejected as illegal. This combined with an upstream HTTP proxy that doesn't parse such `Content-Length` headers, but forwards them, can result in "request smuggling" or "desync attacks". The flaw exists in all prior versions of hyper prior to 0.14.10, if built with `rustc` v1.5.0 or newer. The vulnerability is patched in hyper version 0.14.10. Two workarounds exist: One may reject requests manually that contain a plus sign prefix in the `Content-Length` header or ensure any upstream proxy handles `Content-Length` headers with a plus sign prefix.	2021-07-07	not yet calculated	CVE-2021-32715 MISC CONFIRM
samsung -- bluetooth	Improper privilege management vulnerability in Bluetooth application prior to SMR July-2021 Release 1 allows untrusted application to access the Bluetooth information in Bluetooth application.	2021-07-08	not yet calculated	CVE-2021-25429 MISC
samsung -- bluetooth	SQL injection vulnerability in Bluetooth prior to SMR July-2021 Release 1 allows unauthorized access to paired device information	2021-07-08	not yet calculated	CVE-2021-25427 MISC
samsung -- bluetooth	Improper access control vulnerability in Bluetooth application prior to SMR July-2021 Release 1 allows untrusted application to access the Bluetooth information in Bluetooth application.	2021-07-08	not yet calculated	CVE-2021-25430 MISC
samsung -- caeralyzer	Improper access control vulnerability in Cameralyzer prior to versions 3.2.1041 in 3.2.x, 3.3.1040 in 3.3.x, and 3.4.4210 in 3.4.x allows untrusted applications to access some functions of Cameralyzer.	2021-07-08	not yet calculated	CVE-2021-25431 MISC
samsung -- factorycamerafb	Improper access control vulnerability in FactoryCameraFB prior to version 3.4.74 allows untrusted applications to access arbitrary files with an escalated privilege.	2021-07-08	not yet calculated	CVE-2021-25440 MISC
samsung -- knox_manage	Improper MDM policy management vulnerability in KME module prior to KCS version 1.39 allows MDM users to bypass Knox Manage authentication.	2021-07-08	not yet calculated	CVE-2021-25442 MISC
samsung -- members	Information exposure vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to access chat data.	2021-07-08	not yet calculated	CVE-2021-25432 MISC
samsung -- members	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause arbitrary webpage loading in webview.	2021-07-08	not yet calculated	CVE-2021-25439 MISC
samsung -- members	Improper access control vulnerability in Samsung Members prior to versions 2.4.85.11 in Android O(8.1) and below, and 3.9.10.11 in Android P(9.0) and above allows untrusted applications to cause local file inclusion in webview.	2021-07-08	not yet calculated	CVE-2021-25438 MISC
samsung -- message	Improper component protection vulnerability in SmsViewerActivity of Samsung Message prior to SMR July-2021 Release 1 allows untrusted applications to access Message files.	2021-07-08	not yet calculated	CVE-2021-25426 MISC
samsung -- packagemanager	Improper validation check vulnerability in PackageManager prior to SMR July-2021 Release 1 allows untrusted applications to get dangerous level permission without user confirmation in limited circumstances.	2021-07-08	not yet calculated	CVE-2021-25428 MISC
samsung -- tizen	Improper input validation vulnerability in Tizen FOTA service prior to Firmware update JUL-2021 Release allows arbitrary code execution via Samsung Accessory Protocol.	2021-07-08	not yet calculated	CVE-2021-25436 MISC
samsung -- tizen	Improper access control vulnerability in Tizen FOTA service prior to Firmware update JUL-2021 Release allows attackers to arbitrary code execution by replacing FOTA update file.	2021-07-08	not yet calculated	CVE-2021-25437 MISC
samsung -- tizen	Improper input validation vulnerability in Tizen bootloader prior to Firmware update JUL-2021 Release allows arbitrary code execution using recovery partition in wireless firmware download mode.	2021-07-08	not yet calculated	CVE-2021-25435 MISC
samsung -- tizen	Improper input validation vulnerability in Tizen bootloader prior to Firmware update JUL-2021 Release allows arbitrary code execution using param partition in wireless firmware download mode.	2021-07-08	not yet calculated	CVE-2021-25434 MISC
samsung -- tizen	Improper authorization vulnerability in Tizen factory reset policy prior to Firmware update JUL-2021 Release allows untrusted applications to perform factory reset using dbus signal.	2021-07-08	not yet calculated	CVE-2021-25433 MISC
smartertools -- smartermail	SmarterTools SmarterMail before Build 7776 allows XSS.	2021-07-06	not yet calculated	CVE-2021-32233 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sonicwall -- switch	Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling LLDP Protocol allows an attacker to cause a system instability or potentially read sensitive information from the memory locations.	2021-07-09	not yet calculated	CVE-2021-20024 CONFIRM
suse -- security_incidents	golang/go in 1.0.2 fixes all.bash on shared machines. dotest() in src/pkg/debug/gosym/pclntab_test.go creates a temporary file with predicable name and executes it as shell script.	2021-07-09	not yet calculated	CVE-2012-2666 MISC MISC MISC MISC
suse -- security_incidents	Avahi 0.8 allows a local denial of service (NULL pointer dereference and daemon crash) against avahi-daemon via the D-Bus interface or a "ping .local" command.	2021-07-07	not yet calculated	CVE-2021-36217 MISC MISC
swift -- swift	LengthPrefixedMessageReader in gRPC Swift 1.1.0 and earlier allocates buffers of arbitrary length, which allows remote attackers to cause uncontrolled resource consumption and deny service.	2021-07-09	not yet calculated	CVE-2021-36155 MISC MISC MISC
swift -- swift	Mismanaged state in GRPCWebToHTTP2ServerCodec.swift in gRPC Swift 1.1.0 and 1.1.1 allows remote attackers to deny service by sending malformed requests.	2021-07-09	not yet calculated	CVE-2021-36153 MISC MISC MISC
swift -- swift	HTTP2ToRawGRPCServerCodec in gRPC Swift 1.1.1 and earlier allows remote attackers to deny service via the delivery of many small messages within a single HTTP/2 frame, leading to Uncontrolled Recursion and stack consumption.	2021-07-09	not yet calculated	CVE-2021-36154 MISC MISC MISC
thinksaas -- thinksaas	Improper Authorization in ThinkSAAS v2.7 allows remote attackers to modify the description of any user's photo via the "photoid%5B%5D" and "photodesc%5B%5D" parameters in the component "index.php?app=photo."	2021-07-08	not yet calculated	CVE-2020-18741 MISC
trend_micro -- password_manager	Trend Micro Password Manager (Consumer) version 5.0.0.1217 and below is vulnerable to an Exposed Hazardous Function Remote Code Execution vulnerability which could allow an unprivileged client to manipulate the registry and escalate privileges to SYSTEM on affected installations. Authentication is required to exploit this vulnerability.	2021-07-08	not yet calculated	CVE-2021-32462 MISC MISC
trend_micro -- password_manager	Trend Micro Password Manager (Consumer) version 5.0.0.1217 and below is vulnerable to an Integer Truncation Privilege Escalation vulnerability which could allow a local attacker to trigger a buffer overflow and escalate privileges on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2021-07-08	not yet calculated	CVE-2021-32461 MISC MISC
ubuntu -- atom_perl	It was discovered that the XML::Atom Perl module before version 0.39 did not disable external entities when parsing XML from potentially untrusted sources. This may allow attackers to gain read access to otherwise protected resources, depending on how the library is used.	2021-07-09	not yet calculated	CVE-2012-1102 MISC MISC
vapor -- vapor	Vapor is a web framework for Swift. In versions 4.47.1 and prior, bug in the `Data.init(base32Encoded:)` function opens up the potential for exposing server memory and/or crashing the server (Denial of Service) for applications where untrusted data can end up in said function. Vapor does not currently use this function itself so this only impact applications that use the impacted function directly or through other dependencies. The vulnerability is patched in version 4.47.2. As a workaround, one may use an alternative to Vapor's built-in `Data.init(base32Encoded:)`.	2021-07-09	not yet calculated	CVE-2021-32742 CONFIRM MISC
webkit -- graphicscontext	A use-after-free vulnerability exists in the way Webkit's GraphicsContext handles certain events in WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. A victim must be tricked into visiting a malicious web page to trigger this vulnerability.	2021-07-08	not yet calculated	CVE-2021-21779 MISC
webkitgtk -- webkitgtk	An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.3 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in remote code execution. The victim needs to visit a malicious web site to trigger the vulnerability.	2021-07-08	not yet calculated	CVE-2021-21806 MISC
winwaste.net -- winwaste.net	WinWaste.NET version 1.0.6183.16475 has incorrect permissions, allowing a local unprivileged user to replace the executable with a malicious file that will be executed with "LocalSystem" privileges.	2021-07-08	not yet calculated	CVE-2021-34110 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wordpress -- wordpress	Directory traversal in the CM Download Manager (aka cm-download-manager) plugin 2.7.0 for WordPress allows authorized users to delete arbitrary files and possibly cause a denial of service via the fileName parameter in a deletescreenshot action.	2021-07-07	not yet calculated	CVE-2020-24146 MISC MISC
wordpress -- wordpress	Server-side request forgery (SSR) vulnerability in the WP Smart Import (wp-smart-import) plugin 1.0.0 for WordPress via the file field.	2021-07-07	not yet calculated	CVE-2020-24147 MISC MISC
wordpress -- wordpress	Server-side request forgery (SSRF) in the Podcast Importer SecondLine (podcast-importer-secondline) plugin 1.1.4 for WordPress via the podcast_feed parameter in a secondline_import_initialize action to the secondlinepodcastimport page.	2021-07-07	not yet calculated	CVE-2020-24149 MISC MISC
xyhcms -- xyhcms	A cross site request forgery (CSRF) vulnerability in the /xyhai.php?s=/Auth/editUser URI of XYHCMS V3.6 allows attackers to edit any information of the administrator such as the name, e-mail, and password.	2021-07-08	not yet calculated	CVE-2020-20586 MISC MISC MISC

Back to top